ICT Document No. WhoG-224

ICT Security Incident Response Policy

Version 1.0

10/02/2017

Approved by Executive Director,
Shared Services ICT

Contents

Introduction 5
Purpose 5
Background 5
Audience 6
Scope 6
References 6
Policies 7
Definition of a security event and incident 7
Non-compliance with the ACT PSPF 7
Accountability for security incidents 7
Incident response capability 7
Detecting and responding to security events 7
Automated detection of security events 8
Authority for security incident investigation 8
Authority for investigation 8
Investigations 9
Integrity of evidence 9
Data spills 9
Operation of critical systems 10
Remediating non-compliances 10
Public reporting of security incidents 10
Incident categories 10
External escalation of security incidents 10
Incident response documentation 11
Incident response and investigation training 11
Compliance 11
Roles and responsibilities 12
Appendix A: Incident categories 13
Appendix B: External escalation criteria 14
Appendix C: Incident response and investigation training 15

Introduction

Purpose

The ICT Security Incident Response Policy (SIRP) defines the Territory's approach to detecting and responding to ICT security incidents. The purpose of the SIRP is to ensure when an ICT security event or incident occurs, Shared Services ICT is ready to:

- Identify and record security events and incidents
- Analyse the threat, nature and scope of the incident
- Advise leadership and other stakeholders appropriately
- Minimise spreading or ongoing damage
- Recover affected systems
- Identify actors and preserve evidence
- Educate uses about security awareness
- Identify system vulnerabilities and improve security controls
- Ensure good governance and due diligence
- Protect the Territory's reputation

Compliance with this Standard is *mandatory* for the ACT Government, its employees, contractors and service providers.

Background

The ACT Auditor-General's Office report *Whole-of-Government ICT Security Management and Services* (Report No.2) 2012 recommended Shared Services ICT take a role in "developing whole-of-government policies and procedures for managing ICT security in relation to new technologies". The SIRP fulfils this recommendation, covering technologies such as:

- cloud services
- mobile devices and applications
- production and non-production environments
- metro- and campus-area wifi, and
- network enabled devices.

The SIRP also fulfils the ACT PSPF mandatory requirements under *GOVSEC12 Investigations*, and complies with the ACTPS *Standards for the Conduct of Inquiries and Investigations*.

Audience

The SIRP is primarily written for SSICT to fulfil the requirement of the ACT PSPF for the ITSA to "provide notification and support with relevant stakeholders during major incidents, to ensure collective and holistic responses to the incidents".

Scope

The SIRP applies to all ACT Government employees, agencies, contractors and service providers.

It applies to all security events and incidents related to all Territory ICT applications and infrastructure, whether provided internally or by a private party.

The SIRP excludes service requests and incidents that result from a technical failure of Territory ICT applications or infrastructure.

The SIRP also excludes detailed activities relating to digital forensics. These are covered in the *ICT Security Investigator SOP*.

References

ACTPS *Standards for the Conduct of Inquiries and Investigations* 2010

ACT *Protective Security Policy Framework* (PSPF) 2015

Australian Government *Information Security Manual* (ISM) 2015

Australian Government *Protective security governance guidelines: Reporting incidents and conducting security investigations* 2015

ACT Auditor-General's Office *Whole-of-Government ICT Security Management and Services* (Report No.2) 2012

Policies

Definition of a security event and incident

An ICT security **event** is an identified occurrence of a system, service or network state indicating a possible breach of ICT security policy or failure of controls, or a previously unknown situation that may be relevant to security.

An ICT security **incident** is a single or series of unwanted to unexpected security events that have a significant probability of compromising business operations and threatening information security.

Non-compliance with the ACT PSPF

Any deliberate non-compliance with the ACT PSPF Protocols is to be treated as a security incident and may be treated by the Territory as a breach of the ACTPS Code of Conduct.

Accountability for security incidents

The individual authorising an exception to the ACT PSPF (such as a System Owner who has approved a non-compliance with the recommended security controls for a business system) is accountable for any ICT security incident that arises as a direct result of the exception.

Accountability for ICT security incidents resulting from an exception to the ACT PSPF cannot be attributed to contractors.

Incident response capability

Shared Services will build and maintain the capability to respond to ICT security incidents in a coordinated manner on behalf of agencies.

Instruments

1. Shared Services will implement appropriate processes, training and documentation for ICT Service Desk to collect, record and assign information about ICT security incidents.
2. Shared Services will implement and maintain systems for detecting intrusion attempts, monitoring security events, filtering email, Web and cloud content, and protecting endpoints from malware across all ICT systems, services and devices.
3. Shared Services will maintain systems and capability for performing forensic investigations.

Detecting and responding to security events

All Territory personnel (including Directorate ICT staff) and contractors (including cloud providers) must report any security events they observe within the ICT environment or relating to ACT government information to a coordinating response team.

Instruments

1. All staff and contractors (including cloud service providers) must report ICT security events to the Shared Services ICT Service Desk as soon as possible.
2. ICT Service Desk must respond to all reported security events by:
    a. Recording events in the ITSM system
    b. Assigning security incidents to ICT Security for investigation.
3. ICT Service Desk solutions will be configured to provide additional protection to records of security incidents.

Automated detection of security events

Existing ICT systems, devices and services will be configured to detect and log security events where they have the capability to do so. New ICT systems, devices and services with this capability should be selected on a risk-assessed basis.

Instruments

1. System managers will monitor security events via their logs (ie. regular audits, alerts or other monitoring) to determine when an incident occurs.
2. System managers must report security incidents to ICT Security for analysis and investigation.
3. ICT systems, devices and services with the functionality to automatically detect and log security events should be configured to supply log data to a Security Information and Event Management (SIEM) system on a risk-assessed basis.

   See the *ICT Security Logging and Monitoring Standard* for details.
4. ICT Security will monitor security events via the SIEM system to determine when an incident occurs.

Authority for security incident investigation

The ITSA is the authority for coordinating the investigation of ICT security incidents.

Instruments

1. Initial recording of event details is delegated to the Shared Services ICT Service Desk.
2. Initial analysis is typically delegated to ICT Security Operations to determine full extent, impact and cause of the incident, isolate affected system(s) and coordinate remediation.

Authority for investigation

The ITSA is the authority for initiating an investigation into ICT security incidents. In practice, investigation and reporting is assigned to an accredited ICT Security Investigator or may be delegated to other IT Security Officers (ITSOs) in the ICT Security team.

Instruments

1. The ITSA and the Director of the affected business area are the authority for data discovery.
2. When the incident is likely to relate to a breach of the *ACTPS Code of Conduct*, authorisation from the Director-General or their appointed delegate is required before performing a forensic investigation.

Investigations

The investigation of a reported incident is to be only undertaken by ICT Security or those authorised by ICT Security.

Instruments

1. All activities related to an authorised investigation must be approved by the ITSA or their delegate before they are performed.
2. Investigation activities must be performed in accordance with this ICT Security Incident Response Policy (SIRP).

Integrity of evidence

When investigating an incident, Shared Services, Directorates and service providers must preserve the integrity of evidence.

Instruments

1. All personnel involved in an investigation must maintain a record of actions undertaken to support the investigation.
2. A copy of audit trails relating to an investigation must be transferred to secure file storage for archiving, as well as any manual logs, notes or records.
3. No actions may be performed that affect the integrity of evidence before assisting agencies (such as ASD, AFP or ASIO) are involved.

Data spills

A data spill is an event where Territory data has been accessed or transmitted without authorisation or by persons without an appropriate need-to-know or security clearance, whether maliciously or accidentally.

All Territory personnel and contractors are responsible for reporting any data spills they are aware of to the ICT Service Desk as soon as possible.

Instruments

1. Treat all data spills as an ICT security incident regardless of the cause.
2. Assume the information has been compromised.

3. Report details of the spill to the information owner.
4. Isolate the affected system(s) from the rest of the network.
5. Do not delete information from the affected system(s) until approval is obtained from the ITSA.
6. Do not print or copy the spilled information.

Operation of critical systems

When assessing a security incident related to a GOVERNMENT or BUSINESS CRITICAL system, the ITSA will consult with relevant system owners and system managers about the impact of containment/isolation and possible workarounds for business processes.

Remediating non-compliances

Non-compliance with legislation or agreed security controls discovered in the course of an incident investigation must be remediated by the system owner.

Public reporting of security incidents

Only the agency head may authorise the disclosure of an ICT security incident to the public or media.

Incident categories

To align with the Australian Government, the ACT Government has adopted the Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS). See *Appendix A: Incident Categories* for details.

ISIDRAS is an Australian Government scheme developed by the Australian Signal Directorate (ASD) Information Security Group (ISG) that enables the Australian Government to analyse trends in information security incidents and thus help secure organisations against future incidents.

Categories a rated from 1 to 4. A category 4 incident being the highest and would be of a nature that results in disruption of service.

External escalation of security incidents

ITSOs will report all Category 3 and 4 incidents to ASD's Cyber Security Operations Centre (CSOC). The channel for reporting should be the ICT Security Incident Reporting (CSIR) scheme via the OnSecure website, unless deemed inappropriate for the sensitivity or timeframe of the incident.

See *Appendix B: External escalation criteria* for details of escalations to other recipients.

Incident response documentation

The ITSA is to maintain ICT security procedures.

Instruments:

1. Procedures for detecting and reporting ICT security events
2. Procedures for handling data spills
3. Reporting of ICT security incident metrics to management

Incident response and investigation training

Shared Services will ensure that incident response and forensic investigation training will be provided to ICT security personnel. See *Appendix C: Incident response and investigation training* for details.

Compliance

To comply with this policy:

1. Shared Services will monitor the Territory's ICT security incident response practices and report exceptions to agency heads or their delegates for security.
2. Shared Services will collect ICT security incident response metrics attributed to each agency and report annually to the ACT Government Auditor-General.

Roles and responsibilities

The following positions are responsible, accountable, consulted or informed of security incident response activities.

Table 1: Security incident response RACI matrix

Position	Logging security events	Monitoring security events	Auditing security events	Reporting security events	Security event analysis	Security incident investigation	Investigation coordination	Incident containment	Investigation digital forensics	Incident reporting & escalation	Incident communication
Service Provider	R	R		R			C	R			R
System Owners	A	A	R					A			
Agency head or security delegate			A	A						I	
Staff and contractors				R							I
ITSOs		R		I	R	C	C	C	C	C	
Forensic investigator				I	I	R	R		R	C	
ITSA		A		I	A	A	A	I	A	R	A
Security Executive							I			A	
External stakeholders (law enforcement, etc)										I	

Appendix A: Incident categories

Category 1 Incidents

These include events which cannot definitively be identified as incidents or attacks, and have no effect on system operations such as:

- Isolated and non-repeated scans or pings from an external uncontrolled network.
- Malware detected but removed prior to being placed on an operational system or network.
- Inappropriate content on a machine.
- Abuse of privileges or password confidentiality by agency employee (not extending to superuser or root or administration privileges).

Category 2 Incidents

These also have no effect on system operations, and comprise identified but unsuccessful attempts to actively breach an information system security policy. Such events include:

- Repeated active probes or port mapping from an external network.
- Malware found on a single system but been successfully contained/removed.
- Unsuccessful DOS/DDOS attempts (blocked at external firewall or router).
- Attempt to gain unauthorised access to agency resources, either from within or outside of an Agency network.
- Multiple repetitions of category 1 incidents.

Category 3 Incidents

These include any successful attempt to actively breach an information system security policy on a single system, and may result in a minor or moderate effect on system operations. These could include:

- Unauthorised access by one or more unauthorised people to any account, at any access level.
- Abuse of privileges or password confidentiality by agency employee, extending to super user, root or administration privileges.
- Malware found on more than one system, or inability to contain/remove the code from a system.
- Defacement, alteration or deletion of web server files.
- Successful attack against system services, for example, NIS, DNS, NFS, email, WWW, etc. including denial of service attacks.
- Prank or hoax perpetrated from an external uncontrolled network.
- Unauthorised access to or through a firewall.
- Unauthorised modification to system files and system access controls.
- Unauthorised modification to system hardware or software without the owner's or administrator's knowledge or permission
- National security compromises and disclosures arising from accidental or deliberate breaches of security policy whether intentional or unintentional.

Category 4 Incidents

These include any situation in excess of the examples given above, particularly where high level intervention or crisis management is required. Such incidents will usually have a major effect on system operation.

Appendix B: External escalation criteria

Recipient	Responsibility	Criteria
Affected individuals	Directorate Privacy Officer	An ICT security incident that is also a breach of the IPA will be reported to the affected individual(s) if there is any risk of harm to them as a result of the breach. This notification underpins the ability of affected individuals to restore control over their personal information by changing account names, passwords, contact details etc. It also promotes transparency and trust in ACT Government.
OIAC	Directorate Privacy Officer	An ICT security breach will be reported to the OAIC if it is also a privacy breach.
ASD	ITSA/ITSOs	ASD maintains a database of all ICT security incidents affecting Australian Government agencies, which allows ASD to detect patterns of attacks and forewarn agencies of threats. By contributing full reports about incidents, ACT Government is adding to a body of knowledge that helps protect its own information assets. Further, ASD can be called on to assist with investigation because of its broad knowledge of incidents affecting government ICT. ICT Security will report every ICT security incident to the Director, ASD, via the OnSecure portal or by phone.
AFP	Security Executive	An ICT security incident must be escalated to the AFP if it relates to a criminal matter such as illegal material, theft or threat of violence.
ASIO	Security Executive	An ICT security incident must be escalated to ASIO if it relates to a possible intelligence matter such as a state-sponsored attack or threat of terrorism.
Information partners	Security Executive	An ICT security incident will be reported to an information partner such as the ATO if it relates to the partner agency's data, processes or users.
Public or media	Director-General	The decision to report an ICT security incident to the public or media may only be made by a Director-General.

Appendix C: Incident response and investigation training

Person	Training	Delivery
End users	Security Awareness training including how to detect and report security incidents relating to: • Email, cloud, web browsing and malware • Protective markings and handling sensitive data • Lost, stolen or damaged ICT assets	Induction lecture e-Learning Email bulletins Acceptable Use Policy
Service Desk	Identifying, categorising and recording details of security events How to assign security events to ICT Security	Internal training Knowledgebase
ITSOs	How to analyse security events for system and user behaviour that indicates security incidents have occurred How to safely contain/isolate affected resources How to remediate non-compliant security controls How to collect, preserve and appropriately release evidence of security incidents Digital forensics tools and techniques	ICT industry training Internal training
ITSA	How to coordinate the investigation of security incidents with multiple investigators, service providers and stakeholders How to communicate security incidents to stakeholders How to escalate security incidents the agencies and executives	ICT industry training

Legislation

ACT Criminal Code 2002

ACT Territory Records Act 2002

ACT Information Privacy Act 2014

ACT Workplace Privacy Act 2011

ACT Freedom of Information Act 1989

ACT Public Sector Management Act 1994 (PSMA), including *Public Sector Management Standards*

Electronic Transactions Act 2001

Glossary

Term	Definition
GSO	Government Solicitor's Office
SPOC	Security Point of Contact. Typically a role within a vendor or and agency supporting an ICT system, service or device.
ITSA	IT Security Advisor. This role is currently vested in the Senior Manager, ICT Security, Shared Services ICT.
ITSO	IT Security Officer. Any member of the ICT Security team is delegated by the ITSA with the authority to perform this role.
OAIC	Office of the Australian Information Commissioner
ASD	Australian Signals Directorate

Metadata

Owner	Senior Manager, Shared Services ICT Security
Authority	Executive Director, Shared Services ICT - Executive responsible for ICT Security
Location	KB0001036
Review cycle	This document should be reviewed annually or when relevant change occurs to technology, business or the threat environment.
Associated documents	ACT Government Protective Security Policy Framework ACT Government ICT Security Policy

Approval

Position	Executive Director, Shared Services ICT - Executive responsible for ICT Security
Name	Gary Davis
Signature	
Date	

Revisions

Version	Issued	Amendment details	Author	Approval
0.1	02/06/2016	First draft	S Callahan	
0.2	07/11/2016	Feedback from N Carriage	S Callahan	
0.3	02/11/2016	Feedback from P Major	S Callahan	
1.0	10/02/2017	Ready for publication	S Callahan	

Note: This is a *controlled* document. Any documents appearing in paper form are not controlled and should be checked against the intranet version prior to use.